INFORMATION AND DATA PRIVACY, SECURITY, BREACH AND NOTIFICATION

The Board of Education acknowledges the heightened concern regarding the rise in identity theft and the need for secure networks and prompt notification when security breaches occur. The Board adopts the National Institute for Standards and Technology Cybersecurity Framework Version 1.1 (NIST CSF) for data security and protection. The Data Protection Officer is responsible for ensuring the District's systems follow NIST CSF and adopting technologies, safeguards and practices which align with it. This will include an assessment of the District's current cybersecurity state, their target future cybersecurity state, opportunities for improvement, progress toward the target state, and communication about cyber security risk.

The Board will designate a Data Protection Officer to be responsible for the implementation of the policies and procedures required in Education Law §2-d and its accompanying regulations, and to serve as the point of contact for data security and privacy in the District. This appointment will be made at the annual organizational meeting.

I. Student and Classroom Teacher/Building Principal "Personally Identifiable Information" under Education Law §2-d

A. Definitions

In accordance with Education Law §2-d and/or its implementing regulations, the following terms as used in this policy, are defined as follows:

"*Biometric record*," as applied to student Personally Identifiable Information ("PII"), means one or more measurable biological or behavioral characteristics that can be used for automated recognition of a person, which includes fingerprints, retina and iris patterns, voiceprints, DNA sequence, facial characteristics, and handwriting.

"*Breach*" means the unauthorized acquisition, access, use, or disclosure of student PII and/or classroom teacher or building principal PII by or to a person not authorized to acquire, access, use, or receive the student and/or classroom teacher or building principal PII.

"Directory Information" means information that generally would not be considered harmful if released from a student's record. Directory information, as defined in Policy 5500, is not considered student personally identifiable information.

"*Disclose*" *or "Disclosure"* means to permit access to, or the release, transfer, or other communication of PII by any means, including oral, written, or electronic, whether intended or unintended.

"*Personally Identifiable Information*" (PII), as applied to students, means the following information as concerns District students:

1. Student's name;
2. Name of the student's parent or other family members;

3. Address of the student or student's family;
4. A personal identifier, such as the student's social security number, student number, or biometric record;
5. Other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name;
6. Other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; or
7. Information requested by a person who the District reasonably believes knows the identity of the student to whom the education record relates.

"*Personally Identifiable Information*" (PII) as applied to classroom teachers and building principals means results of Annual Professional Performance Reviews that identify the individual classroom teachers and building principals, which are confidential under Education Law §§3012-c and 3012-d, except where required to be disclosed under state law and regulations.

"*Third-Party Contractor*" means any person or entity, other than an educational agency (i.e., a school, school District, BOCES or State Education Department), that receives student or classroom teacher/building principal PII from the educational agency pursuant to a contract or other written agreement for purposes of providing services to such educational agency, including but not limited to data management or storage services, conducting studies for or on behalf of the educational agency, or audit or evaluation of publicly funded programs. This includes an educational partnership organization that receives PII from a school District to carry out its responsibilities pursuant to Education Law §211-e (for persistently lowest-achieving schools or schools under registration review) and is not an educational agency. This also includes a not-for-profit corporation or other nonprofit organization, other than an educational agency.

For a complete list of statutory and regulatory definitions, please see Education Law §2-d(1)(a)-(k) and the Part 121 Commissioner's Regulations at §121.1.

B. General Provisions

PII as applied to student data is as defined in the Family Educational Rights and Privacy Act (Policy 5125.2), which includes certain types of information that could identify a student, as set forth in Section 1(A) above.

PII as applied to classroom teacher and building principal data, means results of Annual Professional Performance Reviews that identify the individual classroom teachers and building principals, which are confidential under Education Law §§3012-c and 3012-d, except where required to be disclosed under state law and regulations.

The Data Protection Officer will see that every use and disclosure of PII by the District benefits students and the District (e.g., improve academic achievement, empower parents and students

with information, and/or advance efficient and effective school operations). However, PII will not be included in public reports or other documents.

The District will protect the confidentiality of student and classroom teacher/building principal PII while stored or transferred using industry standard safeguards and best practices, such as encryption, firewalls, and passwords. The District will monitor its data systems, develop incident response plans, limit access to PII to District employees and third-party contractors who need such access to fulfill their professional responsibilities or contractual obligations, and destroy PII when it is no longer needed.

Certain federal laws and regulations provide additional rights regarding confidentiality of and access to student records, as well as permitted disclosures without consent, which are addressed in Policy 5125.2 and Regulation 5125.2R, Student Records – Confidentiality and Parental Access to Student Records.

Under no circumstances will the District sell PII. It will not disclose PII for any marketing or commercial purpose, facilitate its use or disclosure by any other party for any marketing or commercial purpose, or permit another party to do so. Further, the District will take steps to minimize the collection, processing, and transmission of PII.

Except as required by law or in the case of enrollment data, the District will not report the following student data to the State Education Department:

1. Juvenile delinquency records;
2. Criminal records;
3. Medical and health records; and
4. Student biometric information.

The District has created and adopted a Parent's Bill of Rights for Data Privacy and Security. It is posted on the District's website at www.kingstoncityschools.org and can be requested from the District Clerk.

C. Third-party Contractors

The District will ensure that contracts with third-party contractors reflect that confidentiality of any student and/or classroom teacher or building principal PII be maintained in accordance with federal and state law and regulations, and this policy.

Each third-party contractor that will receive student data or classroom teacher or building principal data must:

1. Adopt technologies, safeguards and practices that align with the NIST CSF;
2. Comply with the District's data security and privacy policy and applicable laws impacting the District;
3. Limit internal access to PII to only those employees or subcontractors that need access to provide the contracted services;

4. Not use the PII for any purpose not explicitly authorized in its contract;
5. Not disclose any PII to any other party without the prior written consent of the parent or eligible student (i.e., students who are eighteen years old or older):
    a. except for authorized representatives of the third-party contractor to the extent they are carrying out the contract; or
    b. unless required by statute or court order and the third party contractor provides notice of disclosure to the District, unless expressly prohibited.
6. Maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of PII in its custody;
7. Use encryption to protect PII in its custody while in motion or at rest; and
8. Not sell, use, or disclose PII for any marketing or commercial purpose, facilitate its use or disclosure by others for marketing or commercial purpose, or permit another party to do so. Third party contractors may release PII to subcontractors engaged to perform the contractor's obligations, but such subcontractors must abide by data protection obligations of state and federal law and regulations, and the contract with the District.

If a third-party contractor has a breach or unauthorized release of PII, it will promptly notify the District in the most expedient way possible without unreasonable delay, but no more than seven calendar days after the breach's discovery.

D. Third-Party Contractors' Data Security and Privacy Plan

The District will ensure that contracts with all third-party contractors include the third-party contractor's data security and privacy plan. This plan must be accepted by the District.

At a minimum, each third party contractor's data security and privacy plan will:

1. Outline how all state, federal, and local data security and privacy contract requirements over the life of the contract will be met, consistent with this policy;
2. Specify the safeguards and practices it has in place to protect PII;
3. Demonstrate that it complies with the requirements of Section 121.3(c) of the Commissioner's Regulations concerning the supplement to the Bill of Rights;
4. Specify how those who have access to student and/or classroom teacher or building principal data receive or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access;
5. Specify if the third-party contractor will utilize subcontractors and how it will manage those relationships and contracts to ensure personally identifiable information is protected;
6. Specify how the third-party contractor will manage data security and privacy incidents that implicate personally identifiable information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify the District;
7. Describe if, how and when data will be returned to the District, transitioned to a successor contractor, at the District's direction, deleted or destroyed by the third-party contractor when the contract is terminated or expires.

E. Training

The District will provide annual training on data privacy and security awareness to all employees who have access to student and classroom teacher/building principal PII.

F. Reporting

Any breach of the District's information storage or computerized data which compromises the security, confidentiality, or integrity of student or classroom teacher/building principal PII maintained by the District will be promptly reported to the Data Protection Officer, the Superintendent and the Board of Education.

G. Complaints of Breaches or Unauthorized Releases of PII

If a parent/guardian, eligible student, classroom teacher, building principal or other District employee believes or has evidence that student or classroom teacher/building principal PII has been breached or released without authorization, they must submit a complaint in writing to the District. Complaints shall generally be received by the Data Protection Officer, but if a complaint is received by another District employee, such employee must immediately notify the Data Protection Officer. This complaint process will be communicated to parents, eligible students, classroom teachers, building principals, and other District employees.

The District will promptly acknowledge receipt of written complaints, commence an investigation, and take the necessary precautions to protect PII.

Following its investigation of the complaint, the District will provide the complainant with its findings within a reasonable period of time, generally no more than 60 calendar days from the date of receipt of the complaint.

If the District requires additional time, or if the response may compromise security or impede a law enforcement investigation, the District will provide the individual who filed a complaint with a written explanation that includes the approximate date when the District will respond to the complaint.

The District will maintain a record of all complaints of breaches or unauthorized releases of student data and their disposition in accordance with applicable data retention policies, including the Retention and Disposition Schedule for New York Local Government Records (LGS-1).

H. Notification of a Breach or Unauthorized Release of PII

If a third-party contractor has a breach or unauthorized release of PII, it will promptly notify the Data Protection Officer in the most expedient way possible, without unreasonable delay, but no more than seven calendar days after the breach's discovery.

The Data Protection Officer will then notify the State Chief Privacy Officer of the breach or unauthorized release no more than 10 calendar days after it receives the third-party contractor's notification using a form or format prescribed by the State Education Department.

The Data Protection Officer will report every discovery or report of a breach or unauthorized release of student, classroom teacher or building principal data to the Chief Privacy Officer without unreasonable delay, but no more than 10 calendar days after such discovery.

The District will notify affected parents, eligible students, classroom teachers and/or principals in the most expedient way possible and without unreasonable delay, but no more than 60 calendar days after the discovery of a breach or unauthorized release or third-party contractor notification.

However, if notification would interfere with an ongoing law enforcement investigation or cause further disclosure of PII by disclosing an unfixed security vulnerability, the District will notify parents, eligible students, classroom teachers and/or building principals within seven calendar days after the security vulnerability has been remedied or the risk of interference with the law enforcement investigation ends.

Notifications will be clear, concise, use language that is plain and easy to understand, and to the extent available, shall include:

- a brief description of the breach or unauthorized release, the dates of the incident and the date of discovery, if known;
- a description of the types of PII affected;
- an estimate of the number of records affected;
- a brief description of the District's investigation or plan to investigate; and
- contact information for representatives who can assist parents or eligible students with additional questions.

Notification must be directly provided to the affected parent, eligible student, classroom teacher or building principal by first-class mail to their last known address, by email or by telephone.

Where a breach or unauthorized release is attributed to a third-party contractor, the third-party contractor will pay for or promptly reimburse the District for the full cost of such notification.

The unauthorized acquisition of student social security numbers, student ID numbers, or biometric records, when in combination with personal information such as names or other identifiers, may also constitute a breach under State Technology Law §208 if the information is not encrypted, and the acquisition compromises the security, confidentiality, or integrity of personal information maintained by the District. In that event, the District is not required to notify affected people twice, but must follow the procedures to notify state agencies under State Technology Law §208 as outlined in section II below.

II. "Private Information" under State Technology Law §208

A. Definition of "Private Information"

"Private information" is defined in State Technology Law §208, to mean either:

1. Personal information consisting of any information in combination with any one or more of the following data elements, when either the data element or the personal information plus the data element is not encrypted or encrypted with an encryption key that has also been accessed or acquired:

- Social security number;
- Driver's license number or non-driver identification card number;
- Account number, credit or debit card number, in combination with any required security code, access code, password or other information which would permit access to an individual's financial account;
- account number or credit or debit card number, if that number could be used to access a person's financial account without other information such as a password or code; or
- biometric information (data generated by electronic measurements of a person's physical characteristics, such as fingerprint, voice print, or retina or iris image) used to authenticate or ascertain a person's identity; or

2. A user name or email address, along with a password, or security question and answer, that would permit access to an online account.

"Private information" does not include information that can lawfully be made available to the general public pursuant to federal or state law or regulation.

"*Breach of the security of the system*" means unauthorized acquisition or acquisition without valid authorization of physical or computerized data which compromises the security, confidentiality, or integrity of personal information maintained by the District. Good faith acquisition of personal information by an officer or employee or agent of the District for the purposes of the District is not a breach of the security of the system, provided that the private information is not used or subject to unauthorized disclosure.

Any breach of the District's information storage or computerized data which compromises the security, confidentiality, or integrity of "private information" maintained by the District must be promptly reported to the Superintendent and the Board of Education.

B. Procedure for Identifying Security Breaches

In determining whether information has been acquired, or is reasonably believed to have been acquired, by an unauthorized person or a person without valid authorization, the District will consider:

1. Indications that the information is in the physical possession and control of an unauthorized person, such as removal of lost or stolen computer, or other device containing information;
2. Indications that the information has been downloaded or copied;
3. Indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported; and/or

4. Any other factors which the District shall deem appropriate and relevant to such determination.

C. Notification of Breaches to Affected Persons

Once it has been determined that a security breach has occurred, the District will take the following steps:

1. If the breach involved computerized data *owned or licensed* by the District, the District will notify those New York State residents whose private information was, or is reasonably believed to have been accessed or acquired by a person without valid authorization. The disclosure to affected individuals will be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, or any measures necessary to determine the scope of the breach and to restore the integrity of the system. The District will consult with the New York State Office of Information Technology Services to determine the scope of the breach and restoration measures.
2. If the breach involved computer data *maintained* by the District, the District will notify the owner or licensee of the information of the breach immediately following discovery, if the private information was or is reasonably believed to have been accessed or acquired by a person without valid authorization.

The required notice will include (a) District contact information, (b) a description of the categories information that were or are reasonably believed to have been accessed or acquired without authorization, (c) which specific elements of personal or private information were or are reasonably believed to have been acquired and (d) the telephone number and website of relevant state and federal agencies that provide information on security breach response and identity theft protection and prevention. This notice will be directly provided to the affected individuals by either:

1. Written notice
2. Electronic notice, provided that the person to whom notice is required has expressly consented to receiving the notice in electronic form; and that the District keeps a log of each such electronic notification. In no case, however, will the District require a person to consent to accepting such notice in electronic form as a condition of establishing a business relationship or engaging in any transaction.
3. Telephone notification, provided that the District keeps a log of each such telephone notification.

However, if the District can demonstrate to the State Attorney General that (a) the cost of providing notice would exceed $250,000; or (b) that the number of persons to be notified exceeds 500,000; or (c) that the District does not have sufficient contact information, substitute notice may be provided. Substitute notice would consist of all of the following steps:

1. E-mail notice when the District has such address for the affected individual;
2. Conspicuous posting on the District's website, if they maintain one; and

3. Notification to major media.

However, the District is not required to notify individuals if the breach was inadvertently made by individuals authorized to access the information, and the District reasonably determines the breach will not result in misuse of the information, or financial or emotional harm to the affected persons. The District will document its determination in writing and maintain it for at least five years, and will send it to the State Attorney General within 10 days of making the determination.

Additionally, if the District has already notified affected persons under any other federal or state laws or regulations regarding data breaches, including the federal Health Insurance Portability and Accountability Act (HIPAA), the federal Health Information Technology for Economic and Clinical Health (HI TECH) Act, or New York State Education Law §2-d, it is not required to notify them again. Notification to state and other agencies is still required.

D. Notification to State Agencies and Other Entities

Once notice has been made to affected New York State residents, the District shall notify the State Attorney General, the State Department of State, and the State Office of Information Technology Services as to the timing, content, and distribution of the notices and approximate number of affected persons.

If more than 5,000 New York State residents are to be notified at one time, the District will also notify consumer reporting agencies as to the timing, content and distribution of the notices and the approximate number of affected individuals. A list of consumer reporting agencies will be furnished, upon request, by the Office of the State Attorney General.

If the District is required to notify the U.S. Secretary of Health and Human Services of a breach of unsecured protected health information under the federal HIPAA or HI TECH Act, it will also notify the State Attorney General within five business days of notifying the Secretary.

III. Employee "Personal Identifying Information" under Labor Law § 203-d

Pursuant to Labor Law §203-d, the District will not communicate employee "personal identifying information" to the general public. This includes:

1. Social security number;
2. Home address or telephone number;
3. Personal email address;
4. Internet identification name or password;
5. Parent's surname prior to marriage; and
6. Drivers' license number.

In addition, the District will protect employee social security numbers in that such numbers will not be:

1. Publicly posted or displayed;
2. Visibly printed on any ID badge, card or time card;
3. Placed in files with unrestricted access; or
4. Used for occupational licensing purposes.

Employees with access to such information will be notified of these prohibitions and their obligations.

Cross-ref: 1120, District Records
5500, Student Records
8630, Computer Resources and Data Management
4765, Online, Distance, and Remote Learning

Ref: State Technology Law §§201-208
Labor Law §203-d
Education Law §2-d
8 NYCRR Part 121

First Reading: October 7, 2020
Adoption date: October 21, 2020